Published on *LET* (http://let.iiec.unam.mx)

# In Baltimore and beyond, a stolen N.S.A. tool wreaks Havoc

Enviado por SilvanoHdz en Mié, 06/12/2019 - 13:50
**Cita:**

Pearlroth, Nicole y Scott Shane [2019], "In Baltimore and beyond, a stolen N.S.A. tool wreaks Havoc", *The New York Times*, New York, 25 de mayo, https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html [1]

**Fuente:**
Otra
**Fecha de publicación:**
Sábado, Mayo 25, 2019
**Revista descriptores:**
Corporaciones militares - corporaciones civiles que participan en la producción militar o en actividades militares [2]
Formas de la guerra [3]
Relación economía y guerra [4]
Sujetos de la guerra [5]
Tecnologías militares - tecnologías de uso dual [6]
**Tema:**
El comienzo de una ola de ataques cibernéticos en Estados Unidos.
**Idea principal:**

Recientemente se han registrado ciberataques en varias ciudades de Estados Unidos. Baltimore ha sido la principal afectada pero también Texas y Pensilvania. Estos ataques han provocado que los sistemas operativos del gobierno se detengan, que las empresas pierdan ventas y, como consecuencia general, se registran altas perdidas de dinero.

Se trata de ETERNALBLUE, una ciberarma que se creó en la Agencia de Seguridad Nacional (N.S.A, por sus siglas en inglés) de Estados Unidos. En 2017, la N.S.A perdió el control de su creación, de esta manera la herramienta cibernética estuvo viajando por diferentes partes del mundo: se utilizó para generar ataques en Corea del Norte, en Rusia y más recientemente en China. Actualmente, la ciberarma regresó a su lugar de origen y a las autoridades estadounidenses les ha costado mucho trabajo detener a los responsables de los estragos en la red del país norteamericano.

La N.S.A se ha negado a la discusión del tema. La ciberarma fue robada a la institución en 2017 por un grupo que la seguridad nacional no ha logrado identificar, pero los delincuentes se autonombraron Shadow Brokers.

Desde que robaron ETERNALBLUE, agencias de inteligencia foránea y delincuentes individuales han utilizado la herramienta para extender un malware que paralizó hospitales, fábricas y hasta operadores navieros. Sin embargo, la actual crisis de ciberataques en Estados

Unidos tiene como principal objetivo a los gobiernos locales de estados que no cuentan con suficiente tecnología para hacerle frente a los golpes cibernéticos.

Antes de que ETERNALBLUE saliera de las oficinas de la N.S.A era un instrumento invaluable que sirvió para operaciones contra el terrorismo. Los agentes de esta institución lo elaboraron buscando un código de falla en el software de Microsoft, cuando lo encontraron lo llamaron EternalBluescreen. El gobierno estadounidense jamás informó a la empresa que su software era vulnerable, de esta manera los ingenieros de Microsoft jamás hicieron algo para prevenir o evitar las fallas que puede y está causando el uso de ETERNALBLUE en sus equipos.

El primer usuario de ETERNALBLUE fuera de la N.S.A fue Corea del Norte. En 2017, desde el país asiático, se ejecutó el ataque llamado WannaCry para paralizar el sistema de atención médica británico. Posteriormente Rusia atacó a Ucrania, en un ataque que se extendió por todo el país y que apuntaba a las grandes compañías de negocios de la nación, a este acontecimiento se le conoció como NotPetya. En el mismo sentido, los hackers rusos que sabotearon las elecciones estadounidenses de 2016, utilizaron ETERNALBLUE para hacer fallar la red wifi de una cadena de hoteles estadounidenses. Además, Symantec y FireEye, ambas firmas de seguridad, han detectado que piratas informáticos iraníes han utilizado la herramienta para difundir ransomware(1) y hackear aerolíneas de Medio Oriente.

A pesar de que un mes antes de que Shadow Brokers descargara ETERNALBLUE en 2017, la N.S.A avisó a Microsoft y otras compañías sobre las amenazas. Estas empresas de tecnología elaboraron un parche que comenzó a difundirse, sin embargo aún hay cientos de equipos que no cuentan con esta protección. De esta manera, desde julio de 2018 el Departamento de Seguridad Nacional de Estados Unidos emitió una alerta sobre ataques a los sistemas computacionales de los gobiernos locales, esto empezó en Baltimore y San Antonio, después se extendió.

Ante la situación, algunos funcionarios del FBI y de Seguridad Nacional de Estados Unidos, dijeron que la N.S.A debería enfrentar su responsabilidad; ante ello, Michael S. Rogers, director de N.S.A durante los ataques de Shadow Brokers, dijo que la responsabilidad de los ataques no era de la institución, que ellos únicamente habían elaborado una herramienta a la que posteriormente se le dio un mal uso.

En Microsoft se opusieron al argumento del señor Rogers. Ante la situación, la empresa ha solicitado una Convención de Ginebra Digital para gobernar el ciberespacio y lograr una mejor comunicación entre gobiernos y proveedores de tecnología. De hecho Microsoft, Google y Facebook se unieron al Llamado de París para la Confianza y la Seguridad en el Ciberespacio, propuesta ideada por Macron, el presidente de Francia, para comprometerse en lograr que el mundo en línea sea un sitio más seguro. A este llamado no asistieron los ciber atacantes más peligrosos del mundo: China, Irán, Israel, Corea del Norte, Rusia y Estados Unidos, esto nos hace pensar que aún quedan muchos ataques como los del estilo de Baltimore.

---

(1)Ransomware is a type of malware that encrypts files and folders, preventing access to important files. Ransomware attempts to extort money from victims by asking for money, usually in form of cryptocurrencies, in exchange for the decryption key. But cybercriminals won't always follow through and unlock the files they encrypted. Fuente: Ransomware [7]

**Datos cruciales:**

1. El ataque de Baltimore , el 7 de mayo de 2018, fue un asalto clásico de ransomware. Las pantallas de los trabajadores de la ciudad se interceptaron con un mensaje que les exigía 100,000 dólares en Bitcoin para liberar sus archivos.

2. El ataque cibernético, WannaCry, paralizó el sistema de atención médica británico, los ferrocarriles alemanes y unas 200,000 organizaciones en todo el mundo.

3. El ataque NotPetya le costó a FedEx 400 millones de dólares y a Merck, el gigante farmacéutico, 670 millones de dólares.

4. Hasta hace aproximadamente una década, las armas cibernéticas más poderosas pertenecían casi exclusivamente a las agencias de inteligencia. Los funcionarios de la N.S.A usaban el término "NOBUS", que significa: "nadie más que nosotros", para referirse a este tipo de herramientas. Sin embargo, en la actualidad existen muchos casos de robo de este tipo de tecnologías.

**Nexo con el tema que estudiamos:**

La elaboración de armas desde hace mucho tiempo ya no es actividad propia del sistema estatal de un país. Actualmente las tecnologías para la guerra se comercializan y se distribuyen en sitios de fácil acceso. En este sentido, el artículo nos describe una situación en la que el sistema de seguridad de un Estado perdió el control de sus creaciones, ante esto, los hechos que se desencadenaron permitieron a los gobiernos internacionales darse cuenta que es necesario formar un sistema de seguridad internacional para controlar este tipo de situaciones.

---



**Links**
[1] https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html
[2] http://let.iiec.unam.mx/taxonomy/term/72
[3] http://let.iiec.unam.mx/descriptores-let/formas-de-la-guerra
[4] http://let.iiec.unam.mx/descriptores-let/relaci%C3%B3n-econom%C3%ADa-y-guerra
[5] http://let.iiec.unam.mx/descriptores-let/sujetos-de-la-guerra
[6] http://let.iiec.unam.mx/descriptores-let/tecnolog%C3%ADas-militares-tecnolog%C3%ADas-de-uso-dual
[7] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/ransomware-malware